INFORMATION TECHNOLOGY AND HIPAA

INTRODUCTION

Diffusion of Information Technology (IT) throughout the health care delivery system over the last several years has affected the way hospitals and other providers conduct their business. A number of market-driven factors (e.g., a shift of financial risk from payers to providers) explain IT dissemination and the growth of a health care IT "market" that is populated by hundreds of vendors. Prospective payment methods, negotiated discounts, transfer of care to outpatient settings, and demands for documented performance are insurance market changes that have induced hospitals to achieve administrative efficiencies and better outcomes of care. As a consequence, some hospitals are attempting to integrate vertically and horizontally in order to compete successfully. IT is regularly presented as a tool to facilitate this transformation.

New information technologies have:

- helped automate billing and other administrative transactions;
- enabled the storage and transmission of increasing volumes of data among payers, hospitals, and clinicians; and
- generally made financial, administrative and clinical information more readily available to the various parties involved in patient care.

Automation and "connectivity" in health information management is expected to result in administrative efficiencies and improved quality of care. These changes, however, come with additional cost and risk. The initial and on-going cost of investing in IT is substantial, particularly at a time when hospitals are challenged financially. One of the concerns and risks posed by these changes is that third parties could obtain and use individually identifiable health care information inappropriately.

The "Administrative Simplification" provisions of the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 attempt to take advantage of the new possibilities afforded by IT while ensuring the protection of personally identifiable health information. A primary purpose of the law is to decrease system-wide costs by setting common formats for health care transactions between providers and the multiple payers that characterize our fragmented health insurance system. For example, payers, providers and clearinghouses that electronically receive and submit claims must utilize a standard format. Additionally the statute was intended to ensure that the confidentiality of health information, currently protected in varying degrees by state, was also preserved in this new environment.

Automation and information management is expected to result in administrative efficiencies and improved quality of care. These changes come with additional cost and risk.

In sum, health care providers now face regulatory and market-driven demands to examine their day-to-day operations and modify them as needed. The goal is to improve administrative efficiencies and patient quality of care, continue to protect patient confidentiality and, ultimately, survive financially in a constantly changing environment. Information Technology can enable these efforts.

INFORMATION TECHNOLOGY IN HEALTH CARE AND HOSPITALS

Overview

Over the past several decades the need for Information Technology (IT) and its

role in the health care industry has changed drastically. Hospital information systems have evolved from primarily stand-alone mainframes that served the needs of a single organization to a series of complex integrated networks that connect multiple organizations and facilities. Information system applications have evolved from separate "silos" of information to integrated systems to track patients across the continuum of care. Through this evolution, the role and expectations of IT also changed. While

the new demands for IT have certainly driven an increase in the supply of technology and technology vendors, expanding technology capabilities also have raised levels of demand and expectations for IT in all facets of hospital and health care organizations.

Evolution of Need and Capabilities

From a historical perspective, the 1960s are frequently considered the "dawn" of health care computing, with each health care facility typically maintaining its own large mainframe computer that primarily performed financial and admitting functions.[1] In the 1970s, individual stand-alone department systems began to emerge; these created separate pockets, or "silos" of automated information within a facility. For instance, ancillary systems, such as laboratory, became computerized. However, the electronic records were not usually integrated. Instead, the systems printed out the data, which was then stored in a manual record. The 1980s were marked by the introduction of the personal computer (PC) and the continued proliferation of department systems, aided in part by the increased capabilities and tool sets associated with the PC. Integration among the systems was a goal that was difficult to attain.

The 1990s brought significant change to the use of and need for IT. Among the most dynamic changes were the market shift from "fee for service" to managed care which introduced capitation and risk sharing among payers, and changes in government reimbursements. For instance, under the "fee for service" system, health care information systems (HCIS) were mainly used to keep patient accounts, track bill payments, and to provide claims for individuals, the government, and private insurers. As the insurance market shifted towards managed care, payers required that providers supply more information to track results, control costs, and improve outcomes. This required more sophisticated information systems. Hospitals began to grapple with an increasingly competitive and risky environment while at the same time experiencing shrinking revenues. Integration along the continuum of care and mergers/affiliations among hospitals increased dramatically during this period in order to increase revenue, decrease costs, maintain or increase competitive

position, and increase service levels. These changes required changes to IT strategy. Focus shifted from stand-alone department systems to enterprise systems, integrating and providing access to data across a geographically distributed network of organizations. At the same time, market forces also demanded increased operational and administrative efficiencies through better, timely, integrated data, consolidated systems and functions, and the implementation of complex integrated communication networks.

Throughout this evolution, the role and perception of IT changed significantly. At its inception, the IT organization was considered a back-office function, frequently residing in the basement of an organization (near the large computers and wiring systems), and reported to another department within the organizational hierarchy (e.g., finance).[2] Today, IT is typically a separate department led by a Chief Information Officer, who is part of the hospital senior executive team.[3] The role and responsibility of the IT department also changed. Functions, such as telephone system responsibility, shifted from other departments to IT as the role of communications expanded to include the integration of voice, data and imaging. Additional functions, such as Medical Records, were also sometimes added to the IT department's responsibilities. IT became less of a centralized system control function and evolved into that of a facilitator and integrator of distributed systems in addition to maintaining and expanding the basic communication channels. IT was utilized to enhance all hospital operations including patient scheduling, claims administration, supplies procurement and patient record management, and became an intricate part of strategic positioning for the organization. In addition to the increased demands within the hospital and the delivery system, IT was used to meet the increased need for hospital information from diverse external stakeholders, including quality reports for employers, cost information for payers, utilization information for manufacturers, and a variety of health care information for patients and consumers.[4]

Coinciding with increased need for IT from health care providers and increasing capabilities in the technology field, a market of health care information technology (HCIT) vendors emerged and experienced their own fluctuations. According to a Goldman Sachs report, the HCIT market was approximately $11 billion in 1997.[5] In 2000, this market is estimated at $14 billion and is composed of approximately 1,200 suppliers.[6] Suppliers range from small companies that provide system integration and development services to large, multinational corporations that offer a full range of IT services and systems. As changes in the organization of the delivery system occurred and the types of information systems expanded, the supplier market also experienced a growth in mergers and acquisitions. It is estimated that by the year 2001, the top 15 HCIT companies could share as much as 40% of the market, assuming the current rate of consolidations.[7] From a hospital perspective, these HCIT vendor shifts present both opportunity and risk. For instance, the opportunity to buy enterprise-wide integrated systems and one-stop shopping could certainly increase as vendors having

In addition to the increased demands within the hospital and the delivery system, IT was used to meet the increased need for hospital information from diverse external stakeholders, including quality reports, cost information, and utilization information.

products that meet different needs merge together. At the same time, these shifts are also likely to result in fundamental changes in vendor strategic direction, with the possibility of unexpected or undesired effects on the operational strategies of hospitals using these vendors and their systems.

Emerging Clinical and Multi-Product Integration Needs

Today's hospital IT departments face a plethora of challenges in meeting changing expectations and needs. Hospitals experience pressure to acquire the latest technical advances while simultaneously needing to be cautious about their investment in order to balance risk and resources.

Through virtual integration of care providers, the need to warehouse, access and use individual patient's clinical data has increased. This allows providers to track patients across the continuum of care with an expectation of improved service performance and reduced cost. According to a Goldman Sachs survey, clinical systems are expected to experience the highest level of growth and spending of all categories of product growth in 2000-2001, followed next by growth in infrastructure and financial systems.[8] According to a Gartner Report, application areas expecting to experience over 40% growth include Computer-Based Patient Record Systems, Enterprise Scheduling Systems, Document Imaging Management Systems, Disease Management Protocol Systems, and Enterprise Master Patient Index Systems.[9] The expected growth in these areas reflect the need to have sufficient clinical data and to have that data follow a patient throughout the continuum of care through capabilities such as having an Enterprise Master Patient Index to uniquely identify a patient across information systems. These areas are also indicative of other forces affecting hospitals, including the advancing age of our population and the subsequent need to manage chronic disease. The rising need for technologies such as Enterprise Scheduling Systems also demonstrates the trend to connect administrative and clinical systems to reduce administrative cost while improving service levels.

Physician and clinical staff buy-in is critical for success but continues to present a great challenge to hospitals.

Clinical systems are gaining momentum and priority for a number of reasons, including caregivers becoming more computer literate, workstations/PCs becoming more intuitive, increases in ambulatory medicine, and the growing supply of clinical systems.[10] However, widespread acceptance of these systems by the medical community is far from complete. Physician and clinical staff buy-in is critical for success but continues to present a great challenge to hospitals.

As clinical systems become increasingly available, the integration of providers and systems will continue to be a focus. Innovative integration among computer systems and other technologies can offer improved customer service and reduced administrative cost. As an example, "the increasing availability of caller identification information gives hospitals the ability to integrate this information with billing and credit and collection systems to produce 'screen pops' to save time and improve customer service."[11] Another newly emerging trend attempts to improve customer service by providing patient access through the Internet. For instance, most hospitals in Connecticut offer information to patients through their web site. A health system in San Diego is

piloting a project to improve customer service by having customers use the Internet to fill out hospital forms, store their insurance information, and schedule their appointments.[12]

Integration is also expected to increase between computer systems and medical devices. It is expected that some of the next generation devices that people wear, ingest or have implanted will be able to provide direct transmission of patient data into electronic format.[13] Examples of such products include embedded glucose monitors that eliminate the need to draw blood samples, "intelligent" inhalers for doctors to track asthma-patient inhaler use, and microchips that can be swallowed to automatically dispense medicines.[14] Consequently, advances in other fields, such as medical technology, can work in concert with the development of IT in the health care industry. However, both medical and information technology compel hospitals to constantly evaluate their investment decisions and priorities because they require significant initial and on-going commitment of financial and human resources.

Emerging Technologies

Emerging technologies can make integration among information systems feasible and financially viable. As the trend for integrated care systems continues to evolve, these technologies might contribute significantly to this effort by offering a multitude of options for acquiring, maintaining and connecting systems. A brief discussion of some of these technologies follows.

Application Service Providers (ASP)
The use of ASPs reduce the initial expense and time associated with implementing new systems by allowing organizations to "rent" the systems, which are housed and maintained by an ASP. Organizations connect to the ASP through their Internet service provider. Consequently, organizations can access the software and obtain the benefits without having to set up and maintain a computer operation at their own location. ASPs also provide the possibility of connecting providers, payers, and government entities quickly, resulting in lower administrative costs.

XML (Extensible Markup Language)
XML is a computer programming language that allows data to be exchanged among many different systems with relative ease by being a translator that sits between the user and the systems. This technology facilitates data interchange, a core issue with current health care information systems, as integrated health care networks are frequently made up of many different organizations that use their own information systems. With XML it is not necessary for the parties to use the same hardware platform, operating systems, business applications, or database management system.

Supply Chain Management
This technology uses the Internet to reinvent procurement systems and reduce cost through virtual medical superstores. If a hospital is using a sophisticated inventory system or enterprise resource planning (ERP) program that can predict material needs based on historical patterns, an electronic procurement system can automatically reorder supplies without requiring staff time to transmit the paperwork, which reduces administrative costs.

Wireless Networking
This technology allows greater amounts of data to be transmitted faster and without the need to have direct connection with a physical workstation (PC) at a desk.

Since many clinicians who work in health care organizations perform many duties away from their workstations or work areas, this new technology dramatically changes how information systems can be used.

Budget constraints pose a barrier to many of the new technologies, such as Convergence, which requires a substantial capital investment in addition to a large change in IT operations.

Convergence

Convergence creates a network that can handle all of an organization's data, video and voice applications. Users can communicate with remote parties as if they were in the same room. This blending of technologies promises more available bandwidth, simplified network installation and maintenance, faster image transmission and retrieval, better image quality, and unites data, video and voice in one communication network. The key to voice, video and data convergence is significant levels of bandwidth. This means that convergence must be built on a robust networking infrastructure, which is an expensive proposition.

Telemedicine

Telemedicine is the delivery of health care services across distances, as patient data and clinical information are sent between providers allowing the patient to remain in one place. Telemedicine applications typically use telecommunications technology for clinical diagnosis, direct care delivery, patient education and the movement of medical information electronically. This technology can have a dramatic effect on the way health care services are delivered because all providers along the continuum of care can use it. As the use of high-speed telecommunications technology becomes more readily available, this may become a critical tool for rural areas.

These emerging technologies, like all the change factors listed above, promote hospital goals of reduced costs, better outcomes, integrated care systems, and operational efficiencies. They also pose significant challenges to hospitals.

Challenges Facing Hospitals

Hospitals face several challenges in their need to meet the changing demands of the health care market, particularly at a time of decreasing financial resources.

Cost of IT

Investments in Information Technology are frequently expensive, both in the short and long term. Initial investments are needed to purchase application systems, hardware platforms or to replace communication architectures. Implementation services from vendors or independent consultants are also frequently needed in order to manage the large quantity and complexity of new system work. These services are costly. After implementation, hospitals need to continue to invest in the technology through maintenance agreements, upgrades, and on-site maintenance staff. Consequently, these projects require substantial budgets, which are more difficult to justify during distressing financial times. According to an *Inside Health Care Computing* reader survey, budget constraints are the most cited worry of hospital IT executives.[15] Recent expenditures for obtaining Y2K compliance, and anticipated expenditures needed for HIPAA compliance, further aggravate this budget dilemma. For instance, a recent Goldman Sachs report based on a survey of hospital CIOs found that the focus on Y2K delayed other capital projects and created a backlog of IT initiatives. Current forecasts predict that obtaining HIPAA compliance will be even costlier than it was to obtain Y2K compliance. HIPAA and

its requirements are discussed in detail in a later section of this report.

Budget constraints pose a barrier to many of the new technologies, such as Convergence, which requires a substantial capital investment in addition to a large change in IT operations, which also can affect staffing needs. Many hospitals have made significant financial investments to set up separate networking infrastructures for voice, video and data and to train staff on these technologies. It is unlikely that they will be eager or able to justify discarding their existing investments in favor of a consolidated network, even given the potential benefits. In addition, according to a Goldman Sachs report, there is a strong desire for hospitals to stabilize their IT environments following the recent Y2K compliance activity.[16]

In addition to the immediate budget and resource concerns for Y2K, hospitals and other health care institutions have historically been conservative in their IT expenditures relative to other industries. According to *Healthcare Information Technology*, IT products and services account for 2-2 1/2% of health care capital budgets, whereas other industries, such as retailing and financial services, invest approximately 10% of their capital budgets in IT.[17] However, this trend appears to be changing. According to a national hospital survey by Goldman Sachs, 2001 hospital capital budgets are expected to grow 3-10% over capital budgets of 2000.[18] In the long-term, these IT expenditures will enable hospitals to achieve their goals; however, in the short-term, they add to the financial pressures that hospitals are experiencing.

Organizational Challenges

A key obstacle hampering the implementation of new technologies and systems is organizational resistance to the establishment of computer-based patient records. It often difficult to gain the medical staff's acceptance of this, particularly if they are resistant to the use of computers and technologies, such as the Internet in particular, in a patient care setting. For instance, the Healthcare Information and Management System Society reports that "as many as 20 companies are currently developing technology platforms for writing prescriptions online, but a survey revealed that few physicians (19%) are actually very interested in using this application in the future."[19] An American Medical Association study released in spring 2000 confirmed that physicians' interest in using Internet technology as a clinical tool is relatively low.[20] As revealed in the Nursing Workforce Issues section of this report, other clinical staff such as nurses are growing increasingly wary of any administrative duty that takes time away from direct patient interaction and care.

Human Resources

Maintaining sufficient IT resources is another organizational challenge for hospitals. The implementation of new technologies requires time and human resources. Currently the demand for highly qualified information system specialists is at an all time high, and that, coupled with the hospitals' present financial crisis, has created significant IT personnel recruitment and retention problems.[21] A 1997 survey conducted by Hersher Associates found that recruitment and retention of personnel was one of CIOs' greatest concerns.[22] It is common to find organizations that have over 20% vacancy rates in IT positions and many of the current staff do not have the knowledge to support the newer technologies. Hospitals and health care organizations are then faced with a serious issue to solve. They are under severe and immediate pressure to upgrade information systems, link multiple organizations, switch to newly emerging technologies, and comply with strong privacy and security regulations mandated in HIPAA but do not have sufficient internal capacity. Consequently, hospitals sometimes must turn to alternatives of in-house staffing. Consultants are frequently able to fill these roles but can be a costly strategy, especially if used for other than short-term needs. "Outsourcing," whereby an external organization provides IT services and functions to hospitals, is another method for getting IT needs met; this method is on the rise.[23]

Regardless of the specific IT investments that hospitals make, a primary and growing concern they will have is with data security.

Vendor Selection and Management

With the evolution of the health care information technology (HCIT) vendor and product market, many hospitals have reduced their in-house development of applications in favor of purchasing software packages that are already developed and that provide service contracts for upgrades as the market changes. Selecting the best software package and vendor is often a challenge to hospitals that must be concerned not only with how the system will meet the needs of an individual department but also how the system fits into the hospital and integrated network strategy. As discussed previously, this selection process is complicated by mergers and consolidations among HCIT vendors, which may improve the ability to integrate multiple systems but may also, to an extreme, result in the elimination of a system from a vendor's product line.

Investment Decisions

Taken together, financial constraints and HCIT vendor market trends make IT strategy choices very complicated and potentially expensive. Confounding this matter is the extremely fast rate at which technology is changing; by the time an investment is made and implemented newer and better technologies may well have emerged. In addition, hospital-oriented application systems are still fairly specialized so, for example, a system that has a strong financial focus might be less useful for other types of applications. This can generate a battle among hospital departments over product vendors and the strategic direction of the organization. In order to eliminate this internal battle, the IT department must determine how to integrate disparate systems, although this is frequently a costly and complex task.

A large challenge to hospitals is selecting the best in leading technology while being mindful of IT advances that are not yet proven, stable, or cannot possibly meet the expected benefits. According to industry literature, emerging technologies go through what is called a "hype curve." The curve begins with a technology trigger,

rises to a peak of inflated expectations before slumping into a "trough of disillusionment," and then begins a slower, steadier trend upward through a slope of enlightenment and finally to a plateau of productivity.[24] While there is frequently a push to do so, the purchase of IT products and methodologies early in this cycle is likely to fall short of expectations with a resultant devastating impact upon obtaining and maintaining organizational buy-in. According to a Gartner report, Application Service Providers (described previously) are currently at the "peak of expectations" and are moving toward "disillusionment." Other emerging technologies will likely follow this same pattern. Pilot and beta systems, which are still under development or are being used for the first time, often also fall short of expectations and can result in significant cost and schedule overruns. As new products and methodologies are entering the market at an increasing rate, the challenge of determining strategies in which to invest will continue.

Data Security

Regardless of the specific IT investments that hospitals make, a primary and growing concern they will have is with data security, particularly as many of the new technologies utilize the Internet. HIPAA regulations are attempting to address concerns in this area, but until those regulations are finalized and implemented, there will continue to be serious reservations about sending and receiving confidential patient information via the Internet. Another issue related to data security is the storage of patient data. For instance, with the use of Application Service Providers, actual patient data will be stored at the ASP location instead of the hospital. Should Internet access be disrupted or the company go out of business, critical records could be lost. In the highly volatile Internet and IT market, the stability and longevity of vendors should be seriously considered. The importance of ensuring data security is likely to increase with the expansion of data integration and sharing. HIPAA exemplifies the increased focused upon data security as it changes the standards for ensuring the confidentiality of patient information.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Overview

Signed into law on August 21, 1996 by President Clinton, the Health Insurance Portability and Accountability Act (HIPAA), also known as the Kennedy-Kassenbaum Bill, was a bipartisan effort designed to improve continuity (also called "portability") and availability with respect to group health plan coverage and group health insurance provided in connection with employment, and insurance coverage in the individual insurance market (not connected to employment).

HIPAA establishes a single national standard for nine different electronic transactions. Those include health care claims submission, claims attachments, health care payment and remittance advice, and others.

The Health Insurance Portability and Accountability Act does the following:

- establishes broad federal guidelines regarding underwriting practices in both large and small group insurance markets;
- provides new rules to protect certain persons who have lost their group coverage; and
- creates underwriting requirements for self-insured health benefits plans under ERISA.

A further section of the statute, entitled "Administrative Simplification," was designed to reduce the costs and administrative burdens of health care by making possible the standardized electronic transmission of many administrative and financial transactions. The law stipulated the protection of individual's health care information as a requirement of administrative simplification. HIPAA charged the Secretary of Health and Human Services (HHS) to develop standards and requirements for the maintenance and transmission of health information in order to ensure the confidentiality of patients' medical records. These confidentiality regulations apply to health plans, health care clearinghouses, and health care providers.

THE PURPOSE OF HIPAA

HIPAA Regulations Identified[26]

Standards for Administrative and Financial Health Care Transactions
Prior to HIPAA, providers and plans used an estimated 400 different electronic formats with many different data requirements in order to exchange claims, remittance advice, and other transactions.[27] This resulted in unjustifiably high administrative costs.

The health care industry had attempted to develop standards for these electronic transactions on a voluntary basis but was unable to achieve consensus on a single set of standards. After a substantial lobbying effort by the health care industry, Congress included Administrative Simplification provisions in HIPAA. HIPAA establishes a single national standard for nine different electronic transactions.[28] Those include health care claims submission, claims attachments, health care payment and remittance advice, and others.

Security and Electronic Signature
Although standards development organizations (SDOs) have worked on developing standards for health care information security for years, no recognized single standard that includes all of the components required by HIPAA has emerged. Consequently, HHS developed a proposed security standard with input from SDOs and business interests and published this standard in August 1998. The proposed standard is technology neutral (does not require a specific type of technology) and scaleable for the size and complexity of health care organizations.[29]

HIPAA mandates the adoption of new security standards to protect an individual's health information while permitting appropriate access and use of the information by providers, clearinghouses, and health plans. The law also mandates that a new standard for electronic signature be employed when an electronic signature is used in the transmission of a HIPAA standard transaction. The proposed security standard is divided into four categories:

- Administrative Procedures;
- Physical Safeguards;
- Technical Data Security Services; and
- Technical Security Mechanisms.

At a minimum, all health plans, clearinghouses, and health care providers that transmit or maintain electronic health information must protect this information by conducting a risk assessment and developing a security plan. They must also document these activities, keep them current, and provide appropriate security training to their employees.[30]

Privacy
With the increased use of Information Technology in the storage of health care data, patient information has become more

vulnerable to unauthorized disclosures. In addition, the current level of privacy protection provided by law varies greatly by state and type of organization. Therefore, federal standards protecting the privacy of health care information were necessary. With the 1996 passage of HIPAA, the law gave Congress 36 months to pass privacy legislation; otherwise, the law authorized HHS to promulgate final regulations to protect patient privacy. Congress did not meet this deadline and so, on November 3, 1999 the HHS published its proposed standards for "individually identifiable health information." These standards outlined specific rights protecting the privacy of individuals' health information along with the obligations of health care providers, health plans, and health care clearinghouses to ensure the confidentiality of patient data.

This proposed regulation would:[31]

- permit health information to be more readily utilized for treatment and payment purposes;
- under defined circumstances, allow health information to be disclosed without patient authorization for certain purposes (such as research, public health, and oversight);
- require written authorization for the use and disclosure of health information for other purposes; and
- create a set of fair information practices to inform patients how their information is used and disclosed, ensure they have access to information about them, and require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information.

Under the proposed rule, health care providers, health plans, and clearinghouses would be prohibited from using or disclosing medical information without patient authorization or unless specifically permitted by the regulation. Health information becomes protected once the data is electronic and remains protected as long as a health care provider, health plan, or clearinghouse possesses the data. The rule also applies to paper printouts of electronic information but providers who maintain records in paper format only are not subject to these information security or privacy regulations.[32] Because one of the goals of the law was to reduce state variances protecting confidentiality, state laws that are less stringent or are in conflict with HIPAA will be preempted by HIPAA. State laws that are more stringent than HIPAA will still be in effect.[33]

Health care providers, health plans, and clearinghouses would be prohibited from using or disclosing medical information without patient authorization or unless specifically permitted by the regulation.

HIPAA Compliance

Currently, only the regulations for "Standards for Administrative and Financial Healthcare Transactions" have been finalized.[34] All other rules have been proposed (except those noted as being suspended), the comment periods have ended, and the health care industry is awaiting publication of these final rules.

Organizations subject to HIPAA are required to be compliant within 26 months after the publication of the final rule. There are specific penalties for the failure to comply with the regulations as well as for wrongful disclosure of individually identifiable health information. For failure to comply, fines will range from $100 to $25,000 for each violation of a regulation. Criminal penalties for knowingly misusing individually identifiable health information will

include fines up to $250,000 for each offense and up to 10 years in prison.

Implementation Issues

For health care organizations, HIPAA is an enterprise-wide operational issue that will affect every area of their systems. There are legal, regulatory, process, security, and technology aspects to each proposed rule that must be carefully evaluated before an organization can begin its implementation plan. The following details some challenges that the industry faces in complying with the various provisions:

One of the biggest misconceptions about the HIPAA legislation is that technical measures alone will be sufficient for HIPAA compliance.

Security and Privacy Provisions

With regard to health care data, HIPAA distinguishes between privacy and security. Security pertains to the methods that organizations must take to protect their information from internal and external threats. Privacy is viewed from the consumer's perspective of how his/her information is used and disclosed.[35]

HIPAA required that health care entities assess their own security needs and risks, and then devise, implement, and maintain appropriate security measures. Some in the industry, particularly the American Hospital Association (AHA), have asserted that although the statute and its subsequent associated regulations, in principle, can provide greater security and privacy they do not provide baseline criteria for each security requirement; they lack a method for independent compliance assessment; and the timeframe for their implementation is unrealistic and should not proceed until final rules have been published for all provisions of HIPAA.[37]

In defining the privacy of medical records, the proposed regulations identified protected information as that data which identifies the individual, starting from the time that the data becomes electronic and includes any paper versions of this electronic information. They stipulated the entities that are covered by the rules are providers, health plans and health care clearinghouses. They also recognize gaps in HIPAA's authority stemming from its inability to directly regulate many of the business partners, third party administrators, contractors, researchers, or marketing firms that may obtain patient information. HHS has attempted to fill this gap by requiring entities that are covered to apply the provisions to entities with which they contract.[37] HHS' authority to regulate to this level was challenged during the comment period.

Financial

Becoming HIPAA compliant will require significant money and resources. Implementation will require re-designing hospital administrative procedures, assessing compliance gaps, hiring additional personnel, training and educating current staff, purchasing new technologies, reviewing contracts and partnering with new vendors. It is difficult to assess the costs and benefits of HIPAA since it proposes sweeping changes. Estimated costs of implementation vary widely (some as much as two to five times the cost of Y2K) but will surely be in the billions of dollars. The federal government has estimated the five-year conservative cost of the privacy regulation alone to be $3.8 billion.

The privacy and security standards may have a more significant short-term financial impact on hospitals than the requirements for administrative simplification. The privacy rules require technical and operational changes in the use of individually identifiable information, whereas

administrative simplification rules allow hospitals and other providers to contract with clearinghouses to re-format non-standard transactions into the national HIPAA standard transactions.

Procedural
HIPAA's security and privacy provisions, particularly those designating changes in how health information is handled and stored, involve much more than implementing new technology or changes to existing technology. One of the biggest misconceptions about the HIPAA legislation is that technical measures alone will be sufficient for HIPAA compliance. The Health Care Finance Administration (HCFA) has placed heavy emphasis on administrative procedural safeguards. This will involve creating a culture of protecting health information and confidentiality of patient data. This includes organizational changes, policies and procedures, employee training, and physical changes in the workplace to prevent unauthorized disclosure of patient information.[39]

Vendor Related Issues
Many vendors have stepped forth offering "HIPAA compliant" solutions to security as well as information systems. As most of the final rules have yet to be published, providers should be wary of these statements.

The Hospital Study Focus Group on IT and HIPAA identified issues concerning their ability to contract with vendors. Large facilities may be doing business with a vast number of IT vendors at one time (40 or more). Individual vendors may not be entirely forthcoming about their level of preparedness. For example, vendors may claim that their systems are 100% compliant, even though most of the final rules are not yet published. Others acknowledge that they will not introduce systems modifications until HIPAA's final rules are issued, as hospitals cannot require vendors to be HIPAA compliant in the absence of final rules. As many vendor contracts are multi-year, some may be coming up (or have come up recently) for renewal. With the lack of final rules, it is difficult to properly draft vendor contracts.

Human Resource Issues
Most Connecticut hospitals do not have or have not allocated sufficient IT or other resources to implement HIPAA regulations within the required schedule. This is particularly the case for the smaller hospitals that have limited IT resources. All hospitals are facing pressing demands, regulatory and otherwise, which are viewed as more critical short-term priorities. In addition, they have not allocated resources for HIPAA compliance because the final provisions have not yet been promulgated.

Preliminary Assessment of Connecticut Hospitals' Readiness
The Hospital Study Focus Group on IT and HIPAA expressed apprehension about HIPAA's regulations. Unlike the federal government's claim that HIPAA administrative simplification provisions will result in greater efficiencies, focus group participants envisioned few benefits to hospitals and other providers. Instead they stated that HIPAA would impose greater burdens on health care institutions that are already faced with instability and financial distress.

Participants believed that Connecticut might be slightly better off than other states, but that its hospitals are still far from being HIPAA compliant. Physician offices are even less prepared than hospitals, as many are unaware of HIPAA's provisions. Hospitals entering into partnerships with physician groups must educate and assist

physician office management regarding compliance.

Participants believed that hospital managers, particularly in larger institutions, are aware of HIPAA. However, hospitals are faced with other, more immediate demands, and therefore, have not allocated the resources or staff necessary for HIPAA preparedness. To ready themselves for HIPAA, hospitals need to establish an organized committee that will meet regularly and is led by a senior manager with project officer responsibilities. This committee ought to develop a systematic strategy regarding HIPAA issues. Participants believed that the organizations and methods implemented for Y2K compliance could serve as useful models for meeting HIPAA standards.

CONCLUSION

Financial pressures on hospitals brought about by market-driven health insurance changes (e.g., shift to capitated payments, discounted prices) have encouraged the automation of hospital business functions and, to a lesser extent, clinical data management. Vertical and horizontal integration among providers has resulted in the need for integrated systems that work across organizational entities. These changes, coupled with the rapid evolution of technology, have created both opportunities and challenges for hospitals in Connecticut and nationwide.

The benefit of automation and connectivity in an information-intensive industry such as health care is tempered by the risk that confidentiality of personal health care information can be more easily breached. The privacy rule proposed by the federal government attempts to address this concern.

There is general agreement on the goals and long-term benefits of the HIPAA regulations, particularly regarding standardization of formats, code sets, and identifiers for health care transactions, which are expected to simplify administration and reduce costs over time. Compliance with the regulations may ultimately provide the synergy needed for the health care industry to achieve the level of automation other information-intensive industries have achieved. However, short-term costs of implementation of standard formats are a concern for providers and, although some controversy and uncertainty surrounds the privacy rule, all parties agree that implementation of privacy provisions will be costly. The impact of HIPAA implementation is expected to vary by state and organization.

RECOMMENDATIONS

In summer 2000 a focus group was assembled to elicit input from industry personnel on Information Technology and the impact of HIPAA. The group consisted of participants from hospitals, software/IT vendors, the Connecticut Hospital Association and the Attorney General's office. The group's recommendations focused primarily on obtaining HIPAA compliance and are as follows:

- Organizations need to recognize that HIPAA is not just an IT issue. HIPAA has implications for all hospital operations, including policies and procedures, and must be considered an organization-wide project.

Frequently, the hospital's Chief Information Officer (CIO) is assigned responsibility for obtaining compliance. A committee with representation from various hospital areas under the guidance of a project officer from senior management would be a more appropriate structure for this effort. This committee should develop a systematic strategy focused on HIPAA issues.

- More provider education is needed to improve understanding of the overall implications of HIPAA.
- HIPAA regulations should be phased in so that compliance can happen simultaneously across all providers for each final rule. Otherwise, different providers will attain compliance in different areas at different times, increasing confusion and promoting varying levels of compliance.
- Coordination among so many providers is an enormous effort. The State should play a convening role. As overseer, the State could be instrumental in bringing more attention to the need for coordination and encourage participation among health care institutions to advance consensus.

NOTES

[1]Ricci MD, Russell J. *Forty Years in the Making : Has HIT Reached Adulthood?* Online Healthcare Informatics. http://www.healthcare-informatics.com/issues/1997/06_97/shoptalk.htm

[2]Healthcare Information and Management Systems Society, *Guide to Effective Healthcare Information and Management Systems and the Role of the Chief Information Officer*, 3rd Edition, 1998, pages 49-51

[3]ibid

[4]Carter, Joyce, Gray, Patrick. Healthcare Information Technology. http://cci.bus.utexas.edu/research/healthcare.htm, May, 1999.

[5]ibid

[6]Medical and Healthcare Marketplace Guide 1999-2000. *Health Care Information Systems—Industry Evolution.*

[7]ibid

[8]U.S. Goldman Sachs Research. *Y2K Hangover Makes 2000 a Challenge.* Healthcare Information Technology. January, 2000.

[9]Gartner. College of Healthcare Information Management Executives. *High-Growth Healthcare Applications Through 2002.* The Connection. September, 2000.

[10]Healthcare Information and Management Systems Society, *Guide to Effective Healthcare Information and Management Systems and the Role of the Chief Information Officer*, 3rd Edition, 1998, pages 168-169

[11]Healthcare Information and Management Systems Society. *Guide to Effective Health Care Telecommunications.* 1996

[12]Rafter, Michelle. *Back to the Future.* Health and Medicine. Special Report. April, 2000.

[13]Journal of Healthcare Information Management. *Emerging Technologies as a Basis for Healthcare Innovation.* Volume 14, Number 2, Summer 2000.

[14]ibid

[15]Inside Healthcare Computing. *Budgets, Installing Top IS Concerns.* Volume 10, Number 21, September 4, 2000.

[16]U.S. Goldman Sachs Research. *Y2K Hangover Makes 2000 a Challenge.* Healthcare Information Technology. January, 2000.

[17]Carter, Joyce, Gray, Patrick. *Healthcare Information Technology*. http://cci.bus.utexas.edu/research/healthcare.htm, May, 1999.

[18]U.S. Goldman Sachs Research. *Y2K Hangover Makes 2000 a Challenge. Healthcare Information Technology.* January, 2000.

[19]Healthcare Information and Management Systems Society. *HIMSS News, Industry News, Massive e-Health Spending Fails to Spur Physician Use of Internet.* Volume 11, Number 9, September, 2000.

[20]Roniger, Rochelle. *Learning to Love the Web.* Healthcare Business. July 2000.

[21]Healthcare Information and Management Systems Society, *Guide to Effective Healthcare Information and Management Systems and the Role of the Chief Information Officer*, 3rd Edition, 1998.

[22]ibid

[23]Ernst & Young, *In a Field of Force, Trends Shaping the Health Industry*. May, 2000.

[24]Gartner. College of Healthcare Information Management Executives. *The ASP Hype cycle: Disillusionment Has Begun.* The Connection. September, 2000.

[25]Department of Health and Human Services. Federal Registry. Part IV. *Standard for Privacy of Individually Identifiable Information.* 1999.

[26]HIPAA's Administrative Simplification section also addressed the following issues:

Unique Identifiers
HIPAA directs the Secretary of HHS to adopt standards for unique health identifiers for Health plans, Health care providers, Employers, and Individuals. The proposed rule would eliminate the current problems that exist due to non-standardized identifiers. For example, a single health care provider may have different numbers for each program and multiple billing numbers within the same program and this complicates the claims submission process. The standards for the National Health Identifier for Individuals have been suspended after concerns over privacy were expressed in Congress and the media. The concern is due to the perception that "access" to all information on an individual could be obtained through a single identifier. As a result, the development of this standard has been postponed until a federal privacy law that offers recourse to individuals is created.

Code Sets
The proposed rule adopts specific code sets to standardize data elements in claims that specify the diagnosis and treatment of patients. The proposed standard for diagnoses is ICD-9-CM (eventually ICD-10-CM). The proposed standard for procedures is ICD-9-CM, volume 3 for inpatient care, CPT4 for outpatient and physician treatment; HCFA's HCPCS for medical equipment, supplies. For drug codes in pharmacy claims, the FDA's National Drug Code (NDC) is proposed.

[27]Department of Health and Human Services. *Notice of Proposed Rulemaking (NPRM) Standard for Privacy of Individually Identifiable Information.* Impact Analysis.

[28]It is important to note that HIPAA does not require that providers switch to electronic transmission if they are currently submitting on paper. It does stipulate that any healthcare provider who elects to conduct the administrative and financial transactions electronically must comply with these standards.

[29]American Health Information Management Association. Journal of AHIMA. *HIPAA: Understanding the Requirements.* April 2000.

[30]QuadraMed. QuardaMed's Internet Forum on HIPAA Preparedness: Executive Summary. http://www.hipaa-iq.com/summary.

[31]Department of Health and Human Services. Website. Proposed Standards for Privacy of Individually Identifiable Health Information.

[32]QuadraMed. QuardaMed's Internet Forum on HIPAA Preparedness: Executive Summary. http://www.hipaa-iq.com/summary.

[33]Department of Health and Human Services. Website. Proposed Standards for Privacy of Individually Identifiable Health Information.

[34]It was finalized in August 2000.

[35]American Health Information Management Association. Journal of AHIMA. *HIPAA: Understanding the Requirements.* April 2000.

[36]American Hospital Association. Comment letter to HCFA. October 1998.

[37]Department of Health and Human Services. Federal Registry. Part IV. *Notice of Proposed Rulemaking (NPRM) Standard for Privacy of Individually Identifiable Information.* 1999.

[38]ibid

[39]Health Data Management. *The Dawn of HIPAA: What the Health Insurance Portability and Accountability Act Means to You.* April 2000